EMPORIA
City of Emporia

** AGENDA**

City Commission Study Session

Wednesday, September 14, 2016
Conference Room 1AB
516 Mechanic Street
10:30 a.m.

- In-fill Housing Program
- IT Security Policy
- Commission Goals

Joint Luncheon w/NRAB

Tentative Agenda for September 21st City Commission Meeting

- City Commission Reports and Comments
- Consent Agenda
  - Set Bid time and Date for Water Department Meter Readers Pickups.
  - Change Order-Warren Way PV1402.
- Public Comment
  - Proclamation Naming September as Emporia Walk for Hunger Day
  - Proclamation Naming First Week of October as Fire Prevention Week
  - Proclamation Naming Manufacturing Days in Emporia.
- Amendment to Ordinance for Designated Parking on the eastside between the 700-800 Block of Merchant.
- Report from City Manager on City Activities

**If you need accommodations due to a disability to participate in this event, meeting, or activity, or alternative format of written materials contact Shelly Kelley, City of Emporia ADA Coordinator at least 48hours before the event at 620-343-4291 or skelley@emporia-kansas.gov*

EMPORIA
City of Emporia

Memo

TO: City Commission

FROM: Jeff Lynch, Community Development Coordinator

CC: Department Heads

DATE: September 7, 2016

SUBJECT: In-Fill Housing Program

In order to provide more affordable housing and to replace homes that have been demolished over the years in the older neighborhoods, providing an in-fill housing development program could make a great improvement to the City's housing stock. Since 2008, over 120 dilapidated single-family homes have been razed through the demolition program, and through condemnation, creating empty lots.

MODERATE INCOME HOUSING (MIH) PROGRAM

GRANT APPLICATION SUMMARY

Grant Source: Kansas Housing Resources Corporation
Anticipated Grant Requested: $220,000
Units To Be Built: 7 within 3 years
Type of Units: Single-Family, Owner-Occupied

Local Leverage Items- (to be provided by the City)
Lots- City currently owns 5 residential buildable lots;
Waiver of Building Permit Fees;
Bridge Loan (pay initial construction costs, re-paid by grant) 50k – 75k;
Sweat Equity (provided by buyers/owners)

Sweat Equity-
Require minimum number of line items of construction work on the house;
Performed by buyers/owners family and friends under qualified supervisor

Keys to Success-
Contractors willing to bid, supervise;
Buyers with adequate credit willing to live in older neighborhoods, and work on homes;
Price: use program components to make more cost-effective:
Pro-Active: Solicit interest now from potential contractors, buyers and lenders to get indication of participation

MODERATE INCOME HOUSING (MIH) PROGRAM PLAN

Choose locations to build

Solicit Applicants
- How to recruit
- Added Criteria (i.e. work in Emporia Area)

Select House Plan, Size, Style
- Applicant Choice?

Applicants Ranked/Chosen

Lender Referral- not exclusive

Applicant Pre-Qualified at Lender

Agreement Signed- Sale price and other details
- Sweat Equity Commitment
- Do not affect credit rating after this point

Request Bids for House Construction

Construction Supervisor Required- to train/oversee sweat equity

Bid Awarded/ Construction Contract Signed by Applicant, Contractor and City

Construction Completed/ Certificate of Occupancy

Final Appraisal

Applicant Loan Closing at Lender

MIH Possible Sweat Equity Items*

(Labor Only)
Install and finish drywall
Install insulation
Install cabinets
Install roofing felt and shingles
Clean up debris

(Labor and Materials)
Painting
Yard seeding

*All items have been reviewed by City Code Services Office.
*Sweat Equity will be allowed as long as an agreement is in place, and all work is supervised.

Steps to Take Now

Solicit Interest- homebuyers, contractors; Letters of Interest Signed

Write Grant Proposal

City Commission Approval (by Oct. 5th meeting)

Submit Grant Application by October 14, 2016 Deadline

ATTACHMENT A

KANSAS HOUSING

RESOURCES CORPORATION

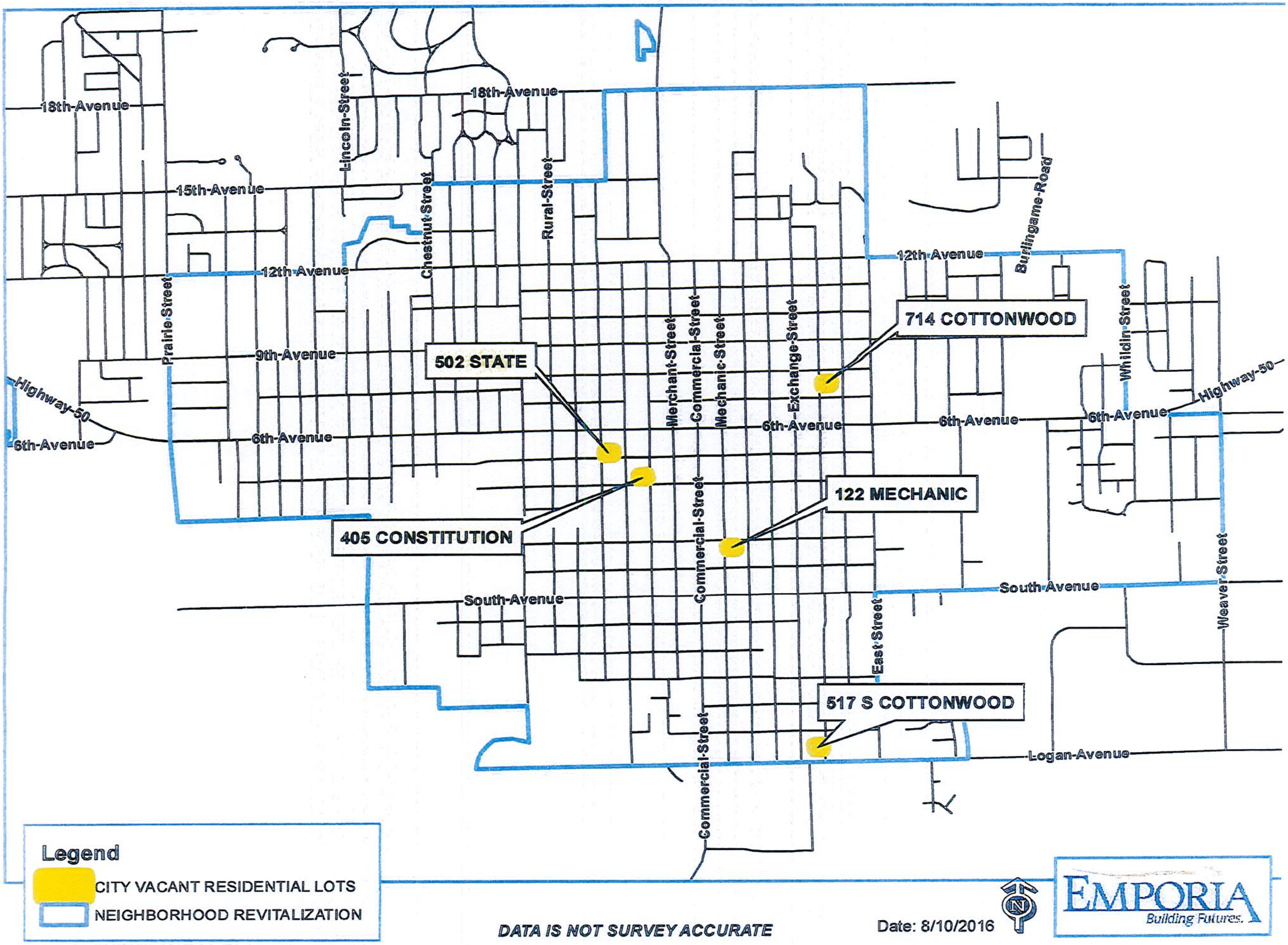
Moderate Income Housing Income Range Guidelines

	1 Person	2 Persons	3 Persons	4 Persons	5 Persons	6 Persons	7 Persons	8 Persons
Maximum	$ 70,031	$ 80,063	$ 90,000	$ 100,031	$ 108,094	$ 116,063	$ 123,281	$ 132,094
Minimum	$ 28,013	$ 32,025	$ 36,000	$ 40,013	$ 43,238	$ 46,425	$ 49,313	$ 52,838

Based upon HUD FY 2016 State Income Summary

Housing Development Program Cash Analysis

Action	Income	Expense	Balance
Grant Award	220,000		220,000
build house #1		120000	100,000
sell house #1	90000		190,000
build house #2		120000	70,000
sell house #2	90000		160,000
build house # 3		120000	40,000
sell house #3	90000		130,000
build house #4		120000	10,000
sell house #4	90000		100,000
build house #5		120000	-20,000
sell house #4	90000		70,000
build house #6		125000	-55,000
sell house #6	90000		35,000
build house #7		125000	-90,000
sell house #7	90000		0
expenses for houses #6 and #7 include land			



DATA IS NOT SURVEY ACCURATE

Date: 8/10/2016

EMPORIA
Building Futures.

502 State

08/26/2016

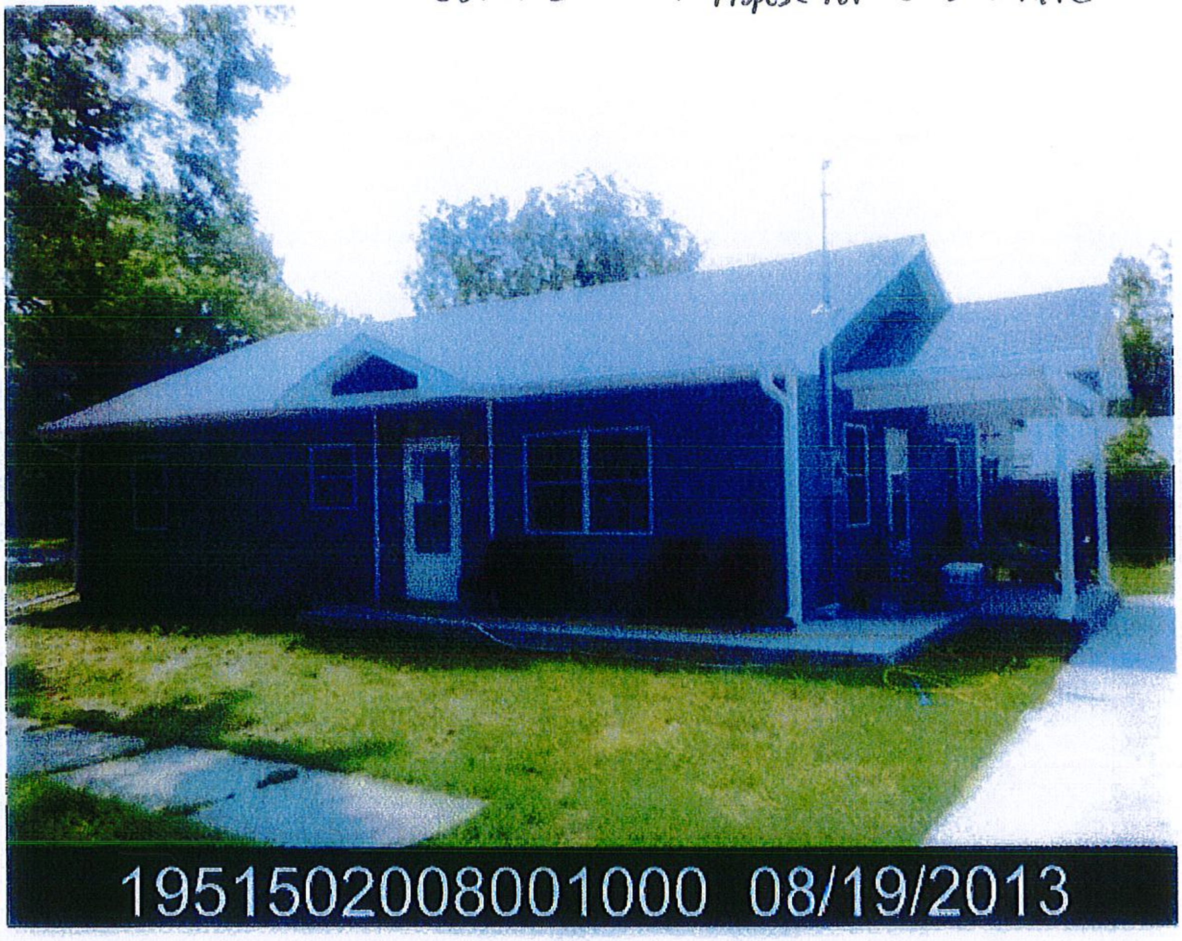
STATE ST.
W. 5TH AV
08/26/2016

08/26/2016

E ST.
AV
08/26/2016

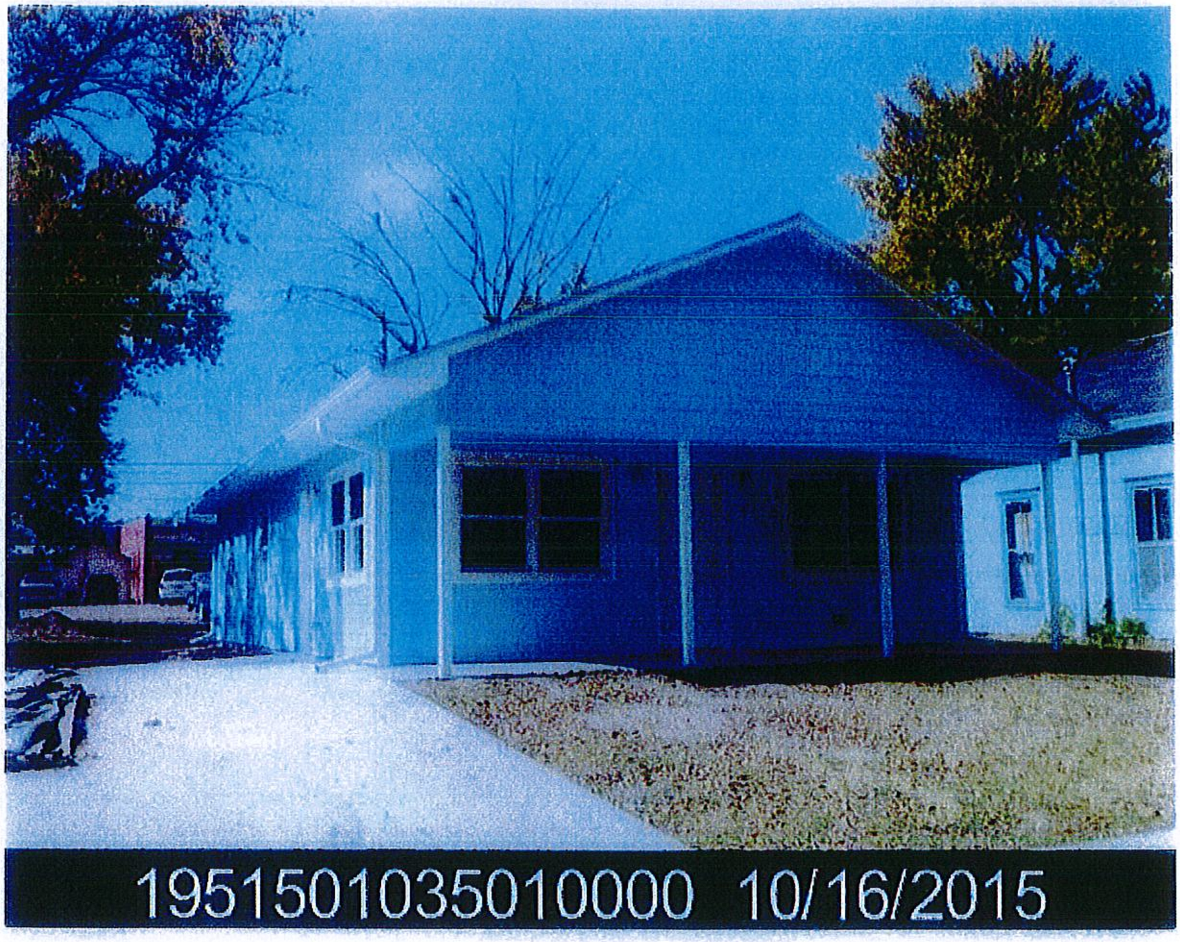
517 S. Cottonwood 75x130

601 W 5th → Propose for 502 State



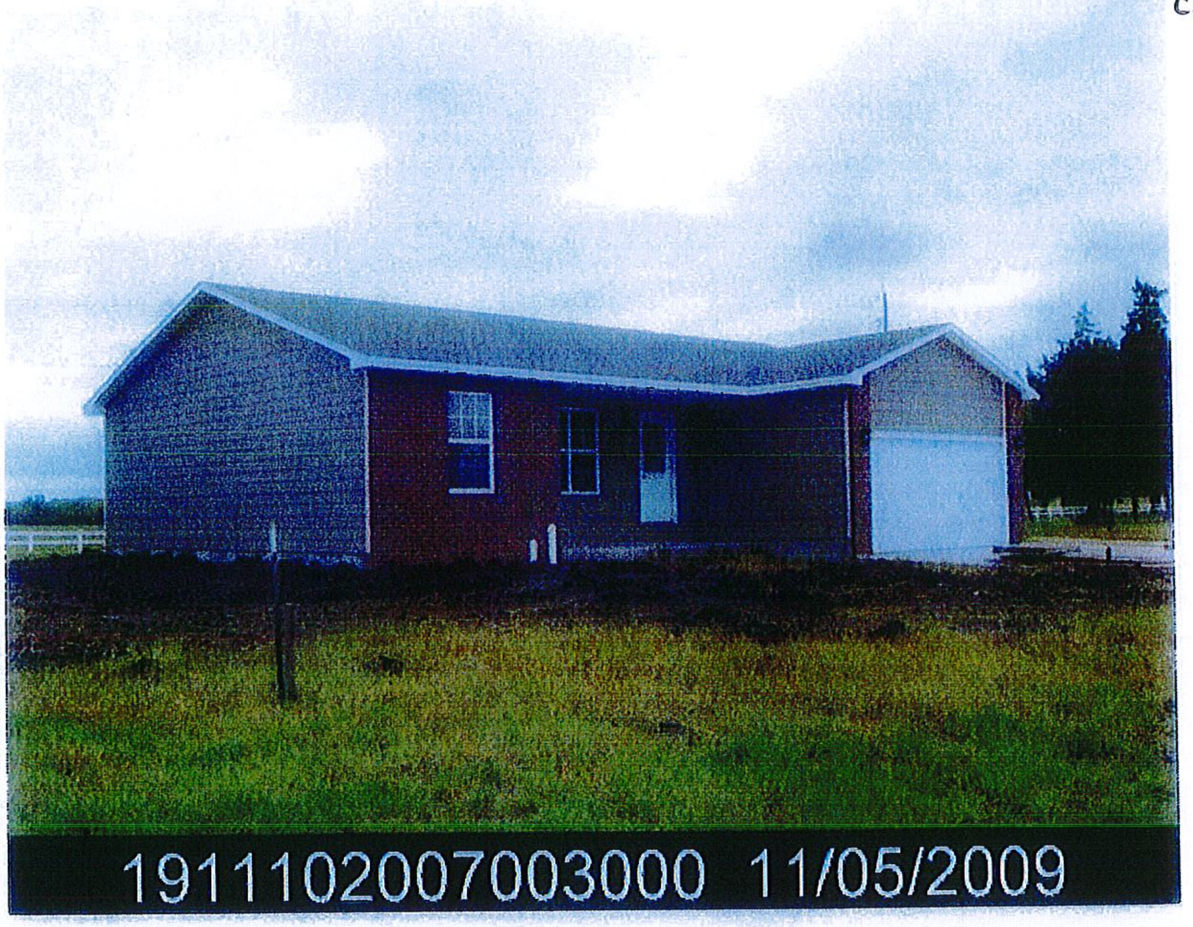
1,320 Sq. Ft.
3 Bedrooms
1 Bath
Slab

117 Mechanic



1,092 Sq. Ft.
3 Bedrooms
1 Bath
Slab

1339 Buffalo Terr. → Propose for 517 S. Cottonwood



1911102007003000 11/05/2009

1,216 Sq. Ft.

3 Bedrooms

2 Baths

Full Basement

https://beacon.schneidercorp.com/PhotoEngine/Photo/237/1911102007003000/1/0.jpg 8/31/2016

EMPORIA
City of Emporia

Memo

TO: City Commission

FROM: Jim Witt, Assistant City Manager

CC: Department Heads

DATE: September 7, 2016

SUBJECT: IT Security Policy

The IT Security was compiled by our staff and members of that division will be on hand to review it with the Commission. Staff will also review recent actions related to City/County cooperation in the IT area.

EMPORIA

City of Emporia

Security Strategy

9/08/2016
Version 1.0

EMPORIA
City of Emporia

Security Strategy

Security Strategy

A methodology for defining security policies and controls

- **Predict Attack / Assess Risk**
  - **For each type of threat (e.g., malicious attacker)**
    - **For each type of method of attack (e.g., virus)**
      - **Proactive strategy**
        - Predict possible damage
        - Determine vulnerabilties
        - Minimize vulnerabilities
          - Implement plan and develop security policies and controls
        - Make contingency plans
      - **Reactive strategy**
        - Assess damage
        - Determine the cause of damage
        - Repair damage
          - Implement plan and develop security policies and controls
        - Document and learn
        - Implement contingency plan
- **Review Outcome / Do Simulation**
- **Review Policy Effectiveness**
- **Adjust Policy Accordingly**

Predict Attack/Assess Risk

It is impossible to defend against all attacks, so it is important to determine the attacks that are most likely to happen and find ways to prepare and defend against these attacks. It is best to prevent or minimalize an attack rather than repair the damage after one has occurred. In order to minimize attacks, it is important to get an understanding on how each attack works and the effect it can have on a system. The various variables of an attack can be shown in the following equation:

Threats + Motives + Tools and Techniques + Vulnerabilities = Attack

A threat is an individual who attacks a system. A threat could be a malicious person such as a disgruntled employee or an outsider (crackers, hackers, etc.). A threat can also be a careless employee who left their computer unlocked or has accidentally downloaded malware. A careless employee, however, does not involve a motive.

A motive is a goal that an attacker strives to achieve. The motive could be anywhere from an attacker trying to steal information or money to an attacker simply trying to break into a system to test their skills.

A tool or technique is used by an attacker to aid them in breaking into a system.

A vulnerability is a flaw in a system that an attacker uses to get into a system. **Most vulnerabilities are preventable by making sure the software and operating system is up to date.** There are flaws in every program and operating system. Some are discovered and patched up by developers and some are discovered by attackers that use the flaw to their advantage.

Type of Threats

1) Security Threats
    a) Natural Disasters
        i) Floods, Fires, Tornadoes, Earthquakes, etc.
    b) Human
        i) Non-Malicious
            (1) Ignorant or careless employees.
        ii) Malicious
            (1) Outsiders (crackers or attackers)
            (2) Insiders (Disgruntled Employees)

There are numerous methods for an attacker may use. The following is a list of some of the most common attacks.

- Denial of service attacks
- Intrusion attacks
- Social engineering
- Viruses
- Worms
- Trojan horses
- Packet replay
- Password cracking
- E-mail cracking
- Ransomware

Proactive Strategy

The proactive strategy is a set of steps used to prevent attacks before they happen. These steps look at how an attack could damage a computer system and the vulnerabilities it exploits. The knowledge gained from a proactive strategy will help in creating and editing security policies. There are three steps of the proactive strategy.

1. Determine the damage that the attack will cause.

2. Determine the vulnerabilities and weaknesses that the attack will exploit.

3. Minimize the vulnerabilities and weaknesses that are determined to be weak points in the system for that specific attack.

Following these steps once an attack happens has many benefits. A pattern will begin to emerge because of the many factors that overlap for different attacks. This pattern is helpful to determining the areas of vulnerability that are the greatest risk for a company.

Determine Vulnerabilities

Possible damages to a system can range from minor glitches to huge data loss. Determining the type of attack, threat, and method makes it easier to discover existing vulnerabilities. The following is a list of possible vulnerabilities:

Physical Security:

- Are there locks and entry procedures to gain access to servers?
- Is there sufficient air conditioning and are air filters being cleaned out regularly? Are air conditioning ducts safeguarded against break-ins?
- Are there uninterruptible power supplies and generators and are they being checked through maintenance procedures?
- Is there fire suppression and pumping equipment, and proper maintenance procedures for the equipment?
- Is there protection against hardware and software theft? Are software packages and licenses and backups kept in safes?
- Are there procedures for storing data, backups, and licensed software off-sire and onsite?

Data Security:

- What access controls, integrity controls, and backup procedures are in place to limit attacks?
- Are there privacy policies and procedures that users must comply to?
- What data access controls (authorization, authentication, and implementation) are there?
- What user responsibilities exist for management of data and applications?
- Have direct access storage device management techniques been defined? What is their impact on user file integrity?
- Are there procedures for handling sensitive data?

Network Security:

- What kinds of access controls (Internet, wide area network connections, etc.) are in place?
- Are there authentication procedures? What authentication protocols are used for local area networks, wide area networks and servers? Who has the responsibility for security administration?
- What type of network media, for example, cables, switches, and routers, are used? What type of security do they have?
- Is security implemented on file and print servers?
- Does your organization make use of encryption and cryptography for use over the Internet, Virtual Private Networks (VPNs), e-mail systems, and remote access?
- Does the organization conform to networking standards?

Minimize Vulnerabilities

Minimizing a system's vulnerability and weakness is the first step in developing an effective security policy. By minimizing vulnerabilities, security personnel can minimize the likelihood of an attack, and its effectiveness if one occurs. It is important to not implement too stringent of a plan because the availability of information could become a problem. There must be a balance between security controls and access to information.

Make Contingency Plans

A contingency plan should be made in case of an attack breaks into the system and damages data or other assets that are critical to normal operations. The ultimate goal of a contingency plan is to maintain availability, integrity, and confidentiality of data.

There should be a plan per type of attack and/or per type of threat. Each plan consists of a set of steps to be taken in the event that an attack breaks through the security policies. The contingency plan should:

- Address who must do what, when, and where to keep the organization functional.
- Be rehearsed periodically to keep staff up-to-date with current contingency steps.
- Cover restoring from backups.

- Discuss updating virus software.
- Cover moving production to another location or site.

The following points outline the various evaluation tasks that should be evaluated to develop a contingency plan:

- Evaluate the organization's security policies and controls to accommodate any opportunities found for minimizing vulnerabilities. The evaluation should address the organization's current emergency plan and procedures, and their integration into the contingency plan.
- Evaluate current emergency response procedures and their effect on the continuous operation of business.
- Develop planned responses to attacks and integrate them into the contingency plan, noting the extent to which they are adequate to limit damage and minimize the attack's impact on data processing operations.
- Evaluate backup procedures, including the most recent documentation and disaster recovery tests, to assess their adequacy, and include them in the contingency plan.
- Evaluate disaster recovery plans to determine their adequacy in providing a temporary or longer term operating environment. Disaster recovery plans should include testing the required levels of security so that security personnel can see if they continue to enforce security throughout the process of recovery, temporary operations, and the organization's move back to its original processing site or to a new processing site.

Draw up a detailed document outlining the various findings in the above tasks. The document should list:

- Any scenarios to test the contingency plan.
- The impact that any dependencies, planned-for assistance from outside the organization, and difficulties in obtaining essential resources will have on the plan.
- A list of priorities observed in the recovery operations and the rationale in establishing those priorities.

A reactive strategy is implemented when the proactive strategy for an attack has failed. It defines the steps to be taken during or after the attack.

Assess the Damage

Determine the damage that was caused during the attack. This must be done as quick as possible so that operations can resume.

Determine the Cause of Damage

To determine the cause of damage, it is important to understand what the attack was aimed at and the vulnerabilities that were exploited to gain access. Review system logs, audit logs, and audit trails to discover where the attack originated and the resources that were affected.

Repair the Damage

It is important to restore any damage as quickly as possible to restore normal business operations. The organization's disaster recovery plans and procedures should be efficient enough to cover the restore strategy.

Document and Learn

Once an attack has taken place, it is important to document it. The documentation should cover all aspects of the attack that are known. It should include the damage caused (hardware, software, data loss, loss in productivity), the vulnerabilities and weaknesses that were exploited during an attack, the amount of time and production lost, and the procedures taken to repair the damage.

Implement Contingency Plan

If a contingency plan is already in place, it can be implemented to save time and to keep business operations functioning correctly. If there is no plan, then it is important to develop one based on the documentation from the previous step.

Review Outcome / Do Simulations

Once an attack has happened, review the attack's outcome to the system. This review should include loss in productivity, data or hardware lost, and time taken to recover. If possible, track where the attack originated from, what methods were used to launch the attack, and what vulnerabilities were exploited. Do simulations in a test environment to gain best possible results.

Review Policy Effectiveness

If a policy is in place for defending against an attack that has taken place, they should be reviewed and checked for their effectiveness. If no policy exist, then new ones must be drawn up to minimize or prevent future attacks.

EMPORIA

City of Emporia

Security Policy

9/08/2016

Version 1.0

EMPORIA
City of Emporia

Security Plan: City of Emporia

This plan was developed by the City of Emporia I.T. Department.

Objectives

Our main objective is to prevent security risks in our network with as little cost as possible.

This security plan is our first. We will take a broad view of the security risks facing our network and take prompt action to reduce our exposure. We hope that by taking a wider view, we may be able to plan for threats we don't know about yet.

Circulation

Because this document contains important security information, it is confidential. The following people are authorized to view this document:

- City Manager
- Assistant City Manager
- IT Staff
- Human Resources

IT Staff

Aric Kenyon – Senior IT Technician

Scott Price – Police Department Senior IT Technician

Bradley Hinderliter – IT Technician

Our Network and Systems

City

- **Desktops**:123
- **Laptop computers**: 58
- **Servers**: 16 physical, 19 virtual
- **Switches**:39
- **NAS**: 2
- **Access Points**: 31
- **Firewall**: 3
- **Internet connection**: 100 MB from ValuNet

All the network is connected via Cat5e, fiber, Wi-Fi, or Microwaves.

Security

We compared each computer against the checklist in the Security Guide for Small Business. We also ran the MBSA (Microsoft Baseline Security Analyzer). These actions have given us what security features that we want to focus on:

- **Virus protection**: All computers have Sophos antivirus and Malware Bytes Corporate version. The Malware Bytes is controlled via a central console and IT can initiate a scan on any computer on the network at any time.

- **Spam-filtering software**: Email is through hosted service. Microsoft is in charge of the spam filtering.

- **Firewall**: Cisco Meraki. We just put it in use in 2016 and are in a four-year plan to replace it.

- **Updates**: Every Windows system should be up to date.

- **Passwords**: All users are required to have passwords for their computers.

- **Physical security**: All computers have a City of Emporia sticker on the case and is recorded into our inventory database. Refer to our Server Room Policy for access to our server room.

- **Wireless networking**: We are currently in the process of switching our access points to Cisco Meraki. The Meraki enables us to monitor usage of anyone connected to our wireless network and gives us a more granular control. Our only encryption method is WPA2. We have 2 encrypted SSIDs: Emporia Wireless and LCECC. We have 6 open SSIDs: WLW Auditorium, Emporia Municipal Golf Course, David Traylor Zoo, Emporia Municipal Airport, Public Works, and EFD st2.

- **Web browsing**: With the help on our new firewall, we were able to put heavier restrictions on web browsing.

- **Backups**: All servers are being backed up to our Unitrends Agent in our server room and once a week, all servers are archived out to a NAS sitting in a building at our tower by Public Works.

Risks

We believe the risks break down into four main categories:

- Intruders (viruses, worms, hijacking of our computer resources or Internet connection, and random malicious use). These are the risks that anyone using computers connected to the Internet faces. High risk, high priority.

- External threats (rivals, disgruntled ex-employees, bad guys after money, and thieves). They are likely to use the same tools as hackers, but in deliberately targeting us they may also try to induce members of staff to supply confidential information or even use stolen material to blackmail or damage us. We need to protect our assets with physical and electronic security. High risk, high priority.

- Internal threats. Whether accidental or deliberate, a member of staff may misuse his or her privileges to disclose confidential information. Low risk, low priority.

- Accidents and disasters. Fires, floods, accidental deletions, hardware failures, and computer crashes. Low risk, medium priority.

Priorities

1. Intruder deterrence:
   - Firewall
   - Virus and Malware protection
   - Ensuring that all computers are configured to be updated automatically
   - Ongoing user education and policies

2. Theft prevention:
   - Keeping all computers password protected
   - Security marking and asset inventory
   - Making sure the all offices are locked after everyone leaves

3. Disaster prevention:
   - Frequent backups with offsite storage
   - Ensure all users save critical files on file server, which is being backed up.
   - Offsite backup of critical paper documents
   - Regularly testing the backups by performing a restore

4. Internal security and confidentiality:
   - Strong password policy and user education
   - Restrict access to servers
   - Ensure all Access Points that are put on the network are approved by IT

Policy Changes

All changes to this will be approved by and enforced by members of the IT Department and the City Manager and/or the Assistant City Manager.

Project Time Line and Responsibilities

Within three years, we plan on making all of our access points Cisco Merakis. Maybe get Cisco Meraki Switches if we have the funding. Meraki devices give us near complete control over the network.

We are on a four year replacement plan for all computers and servers. Each computer we put in will have better performance and security than the previous one.

Response Planning

We have a separate document dedicated to our security strategy and we will follow that.

Ongoing Maintenance and Compliance

Unfortunately, our network is too big to go around every month and make sure all computers are up to date. But we have set all computers to automatically update. As we are called to work on problems with a computer, we will double check to make sure it is up to date. We also come in before or after hours every other month to install updates on all our Windows Servers.

There will be a full, formal review of this plan in early 2017.

EMPORIA

City of Emporia

Server Room Policy

Version 1.0
9/06/2016

EMPORIA
City of Emporia

1. PURPOSE

The purpose of this policy is to ensure a minimum level of security is maintained by all City of Emporia and Lyon County staff that has access to the Server Rooms.

2. ROLES AND RESPONSIBILITIES

2A. IT STAFF

It is the responsibility the IT staff to ensure that this policy is enforced and complied with.

2B. ALL OTHER STAFF WITH RIGHTS TO ACCESS

All staff must be aware of this policy and their obligations therein. It is their responsibility to ensure they carry out their duties in a professional manner while working in the Server Room.

2C. VISITORS

All visitors need to be made aware of this policy and their obligations therein. It is the responsibility of the staff member accompanying the visitor or visitors to ensure they carry out their duties in a professional manner whilst working in the Server Room.

3. CREDENTIAL SYSTEM

3A. POLICY AREA: PERSONNEL SECURITY

Having proper security measures against the insider threat is a critical component for the Criminal Justice Information Services (CJIS) Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted Criminal Justice Information (CJI) including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

3B. PERSONNEL SECURITY POLICY AND PROCEDURES

3C. MINIMUM SCREENING REQUIREMENTS FOR INDIVIDUALS REQUIRING ACCESS TO CJI

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a

NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

(i) 5 CFR 731.106; and/or
(ii) Office of Personnel Management policy, regulations, and guidance; and/or
(iii) agency policy, regulations, and guidance.
Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.
2. All requests for access shall be made as specified by the CJIS Systems Officer (CSO). The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
6. If the person is employed by a Noncriminal Justice Agency (NCJA), the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.
7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI.
8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

3D. PERSONNEL SCREENING FOR CONTRACTORS AND VENDORS

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the Contracting Government Agency (CGA) on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

4. ACCESS TO THE SERVER ROOM

There are three parties that have access to the Server Room: City of Emporia IT staff, City of Emporia Police Department staff, and Lyon County Emergency Communication Center staff.

The Server Room is in a secured location. The primary mechanism for controlling access to the IT Server Room is via proximity reader. There are two doors into the server room.

All staff must be credentialed via process described in section 3.

Staff and visitors must have their identification badge with them at all times. A visitor's pass will be provided by the IT department.

A staff member may only operate their respective equipment unless approved by the department head or supervisor of said equipment. (For example, a City of Emporia IT staff member may not swap out tapes from Police Department equipment unless they have permission from the Police Department IT staff.)

It is the responsibility of the last staff member out of the Server Room to make sure that all doors are securely shut. The door is to remain closed at all times unless prior authorization from IT staff is obtained.

The air conditioned unit for the Server Room must be on 24/7. If a staff member notices it is off, it is their responsibility to contact a member of IT immediately.

If a staff member notices an odd burning smell or an unusual noise coming from a server, it is the responsibility of the staff member to immediately notify an IT staff.

It is the staff member's responsibility to report to IT when they see unauthorized personnel in the Server Room.

It is the responsibility of the staff member to lock their equipment up after use.

It is the responsibility of authorized personnel to make sure all servers are plugged into a battery backup to prevent possible data loss in case of an electrical blackout.

It is the responsibility of authorized personnel to make sure their equipment is in the right area (servers in server racks, etc.).

It is the responsibility of authorized personnel to properly dispose of equipment that is out of commission.

Only authorized users are permitted use Remote Desktop Protocol to remote into a server. If a user is remoting into a server from their desk or at home via VPN, it is their responsibility to safely logout of the remote desktop session once they are done.

5. REVIEW

This policy can be reviewed at any time to assess possible changes. All changes must be agreed upon by IT Staff and approved by Assistant City Manager and/or City Manager.

6. DISCIPLINE

Any violations of this policy will be reported to Human Resources. The violator's supervisor will determine if any further action will be necessary.

EMPORIA
City of Emporia

Memo

TO: City Commission

FROM: Jim Witt, Assistant City Manager

CC: Department Heads

DATE: September 7, 2016

SUBJECT: Commission Goals

Staff will review the status of Commission Goals for the 2015-2017-time period. The attached document is an update of the status on all 7 goals as adopted.

9-14-16

COMISSION GOALS 2015-2017 TIMELINES

GOAL 1 - PROMOTE SINGLE FAMILY HOUSING DEVELOPMENT AND REDEVELOPMENT.

Actions

Review historical study reports for evidence data by end of 2015 calendar year.
Anticipated completion of report for submission as supporting document for RHID is no later than 12-15-15. Completed
Submit final application for RHID approval by 1-15-16. Submitted 1-21-16 to Kansas Department of Commerce. Approved February officially February 8, 2016 with city notification on February 18, 2016.

Subdivision Plat for Hidden Vistas Subdivision was approved in July of 2016. Public Hearing on RHID Implementation was held on 9-7-16. The plat contains 25 buildable lots and a Community Pool. Initial SF home construction should begin late this fall.

GOAL 2 - MAXIMIZE ECONOMIC DEVELOPMENT RESOURCES TO BROADEN OPPORTUNITIES AND STRENGTHEN POSITIVE SYNERGIES FOR RELATED CITY COMMISSION FUNDED ORGANIZATIONS.

Actions

Evaluate each funded organization based on last year's results and demonstrated ability to execute their business plans with measurable outcomes as approved by the commission.
Require each funded organization to submit an annual business plan with measurable outcomes approved by the commission.

Identify 2 metrics for each organization by 12-1-15 *Completed 1-6-16*
Notify of requirements outlined in the Actions for this goal by 2-1-16. *Completed.*
Reminder notice to be sent with 2017 budget requests. *ACM failed to follow thru.*

GOAL 3 - ENHANCED INTER/INTRA GOVERNMENTAL COOPERATION BY MAXIMIZING FACILITY AND HUMAN RESOURCES.

Actions

City management will develop a list of potential cooperative partnerships, e.g. public safety, public works, information technology, human resources, finance, shared facilities and economic development.

These activities will be ongoing thru 9-16. At that time staff in cooperation with county staff will present a list of potential cooperative ventures between public agencies. *Joint Facilities Report presented on 1-13-16. Update in July, 2016.Delayed due to cancellation of Joint*

City/County Meeting now moved to October, 2016

GOAL 4 - INCREASE WATER CAPACITIES AND RESOURCES WHILE MEETING FEDERAL AND STATE MANDATES FOR CITY RELATED INFRASTRUCTURE.

Actions

Preserve and utilize current water rights. Seek
and seek additional water rights.
Finalize wastewater facility plan.
Optimize fiscal monetary resources to preserve existing infrastructure.
Evaluate fiscal resources in anticipation of proposed improvements.
Identify proposed improvements and policy changes for stormwater management.

Compliance timetable for water and sewer systems by 1-16. (May be too aggressive) ***Delayed due to internal issues.***
Comprehensive stormwater management plan by 1-17. No progress
Identify the parameters for existing water rights and preservation of same by 7-16.
Initial discussion to be held on April 13th, 2016.
Identify the availability of additional water rights in East Central Kansas by 8-17.
Discussion on Cottonwood Rights and using said rights scheduled for April 13, 2016.
Ongoing discussions will be held as information becomes available.

GOAL 5 - EXAMINE LOCAL GOVERNMENT OPPORTUNITIES TO ASSIST AND SUPPORT THE MISSION AND GROWTH OF THE EDUCATIONAL TRIAD.

Actions

Request from USD 253, E.S.U. and F.H.T.C. a set of cooperative actions to enhance the educational triad.

Opportunistic Goal

GOAL 6 - ASSESS TECHNOLOGY PROCESSES AND PROGRAMS.

Actions

Explore technology frontier(s) with other public organizations. Develop information technology security plan.

Provide and Executable security plan by 7-1-16 to be presented on 9-14-16.

GOAL 7 - REVIEW CITY BOARD AND ADVISORY COMMITTEE DUTIES, MEMBER

9-14-16

DUTIES AND SELECTION PROCESS.

Actions

Review function and relevance for all fourteen city boards and advisory committees.
Review city board committee recruitment processes including application content and advertising.
Consider revising city board/committee selection process to include interviews of candidates.

Function and relevance review to begin 2-16 and completed by 1-17.
Management staff to begin self assessment by boards and liaisons in April of 2016. Completion anticipated by 9-15-16. Now 10-12-16.

City Board and Committee selection process including interview option.
Begin 9-9-15. *Partially complete including Commission Interview Process. Solicitation of applicant process is being monitored and fine tuned.*